

# SAINTwriter Assessment Report

**October 10, 2008**  
**Scan Completed: October 10, 2008 2:21 PM**  
**Scan Level: content search**  
**Scanner Version: 6.9**

## 1.0 Overview

The following vulnerability severity levels are used to categorize the vulnerabilities:

**CRITICAL PROBLEMS**

Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

**AREAS OF CONCERN**

Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

**POTENTIAL PROBLEMS**

Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

**SERVICES**

Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

## 1.1 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class
host1.domain.com	potential	Potentially sensitive information found in C:/Documents and Settings/JohnDoe /Cookies/www.site.com	Other
host2.domain.com		nothing to report	
host3.domain.com	potential	Potentially sensitive information found in C:/Documents and Settings/FooBar/My Documents/personal.doc	Other
host4.domain.com	potential	Potentially sensitive information found in C:/Documents and Settings/smith/My Documents/friends.pdf	Other
host5.domain.com		nothing to report	
host6.domain.com	potential	Potentially sensitive information found in C:/DataStore/employees.xls	Other
host7.domain.com	potential	Potentially sensitive information found in C:/Documents and Settings/jones/Desktop /receipt.html	Other

host8.domain.com		nothing to report	
host9.domain.com		nothing to report	
host10.domain.com	potential	Potentially sensitive information found in C:/Documents and Settings/All Users /Application Data/Accounting/invoices.xml	Other

## 2.0 Details

The following sections provide details on the specific vulnerabilities detected on each host.

### 2.1 host1.domain.com

**IP Address:** 10.0.0.11  
**Scan time:** Oct 10 14:21:33 2008

#### Potentially sensitive information found in C:/Documents and Settings/JohnDoe/Cookies

**Severity:** Potential Problem

**Impact**

This could lead to a possible leak of sensitive information.

**Resolution**

Consider encoding sensitive information.

**Technical Details**

Service: netbios  
Matched String: 1111222233334444 on line 2

### 2.2 host2.domain.com

**IP Address:** 10.0.0.12  
**Scan time:** Oct 10 14:21:33 2008

nothing to report

### 2.3 host3.domain.com

**IP Address:** 10.0.0.13  
**Scan time:** Oct 10 14:21:33 2008

#### Potentially sensitive information found in C:/Documents and Settings/FooBar/My Documents /personal.doc

**Severity:** Potential Problem

**Impact**

This could lead to a possible leak of sensitive information.

## Resolution

Consider encoding sensitive information.

## Technical Details

Service: netbios

Matched String: 111-22-3333 on line 5

## 2.4 host4.domain.com

**IP Address:** 10.0.0.14

**Scan time:** Oct 10 14:21:33 2008

### Potentially sensitive information found in C:/Documents and Settings/smith/My Documents

**Severity:** Potential Problem

#### Impact

This could lead to a possible leak of sensitive information.

#### Resolution

Consider encoding sensitive information.

#### Technical Details

Service: netbios

Matched String: 444-55-6666 on line 7

## 2.5 host5.domain.com

**IP Address:** 10.0.0.15

**Scan time:** Oct 10 14:21:33 2008

nothing to report

## 2.6 host6.domain.com

**IP Address:** 10.0.0.16

**Scan time:** Oct 10 14:21:33 2008

### Potentially sensitive information found in C:/DataStore/employees.xls

**Severity:** Potential Problem

#### Impact

This could lead to a possible leak of sensitive information.

#### Resolution

Consider encoding sensitive information.

### Technical Details

Service: netbios

Matched String: 777-88-9999 on line 27

## 2.7 host7.domain.com

**IP Address:** 10.0.0.17

**Scan time:** Oct 10 14:21:33 2008

### Potentially sensitive information found in C:/Documents and Settings/jones/Desktop/receipt.html

**Severity:** Potential Problem

#### Impact

This could lead to a possible leak of sensitive information.

#### Resolution

Consider encoding sensitive information.

### Technical Details

Service: netbios

Matched String: 5555666677778888 on line 20

## 2.8 host8.domain.com

**IP Address:** 10.0.0.18

**Scan time:** Oct 10 14:21:33 2008

nothing to report

## 2.9 host9.domain.com

**IP Address:** 10.0.0.19

**Scan time:** Oct 10 14:21:33 2008

nothing to report

## 2.10 host10.domain.com

**IP Address:** 10.0.0.20

**Scan time:** Oct 10 14:21:33 2008

### Potentially sensitive information found in C:/Documents and Settings/All Users/Application Data/Accounting/invoices.xml

**Severity:** Potential Problem

**Impact**

This could lead to a possible leak of sensitive information.

**Resolution**

Consider encoding sensitive information.

**Technical Details**

Service: netbios

Matched String: 4444333322221111 on line 65

Copyright 2001-2008 SAINT Corporation. All rights reserved.